ミックスネットについて : 電子データをシャッフルする方法 (符号と暗号の代数的数理)

AUTHOR(S):

佐古, 和恵; 古川, 潤

CITATION:

佐古, 和恵 ...[et al]. ミックスネットについて : 電子データをシャッフルする方法 (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 1-7

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25252

数理解析研究所講究録 1361 巻 2004 年 1-7

ミックスネットについて
～電子データをシャッフルする方法～

佐古　和恵　古川　潤
NEC インターネットシステム研究所

1. はじめに

ミックスネットは電子投票や匿名通信路を実現する際に用いられる技術である。またミックスネットの電子データをシャッフルするという要素技術が、追跡不可能性が必要な暗号プロトコルやMix and Matchと呼ばれるゼロ知識証明プロトコルの証明テクニックに応用されている。本稿ではミックスネットの研究動向について紹介する。

2. ミックスネットとは

ミックスネットについて厳密な定義を与えている論文は少ない。過去の論文の使われ方を参照すると、ミックスネットとはn個の暗号化された入力 $(C_1, C_2, \ldots, C_n)$ に対して、集合として復号された結果の n 個の復号データ $(M_1, M_2, \ldots, M_n)$ を出力するもので、かつ、各 i について C_i を復号した結果がどの M_j になるかの対応が秘匿されるものを指している。さらに、出力の正当性を保証する verifiability や、出力されないで停止してしまうことを防ぐ robustness などの性質が検討されている。前者の verifiability もどのような形で保証するのかによってバリエーションがある。

3. 電子投票での使われ方

ミックスネットのキラーアプリケーションとして電子投票がある。上記のミックスネットの性質がどのように電子投票で有効に活用されているかについて述べる。電子投票で必要となる要件として

1. 不正投票防止
2. 不正集計防止
3. 投票の秘密保護

の３点が挙げられる。不正投票を防止するためには、投票文に電子署名を付与することが効果的である。これによって、有権者が投票していること、有権者であっても２度以上投票していないことを容易に確認できる。しかしこのままでは投票の秘密が守られない．したがって投票文に直接電子署名を付与するのではなく、暗号化した投票文に電子署名を付与することとする。しかし復号しないと集計できない。そこでミックスネットを経由して、入力と出力の対応がわからないように復号し、その結果を集計することとする。この流れはまさに、現在の紙ベースの不在者投票で行われていることと同じである（図１）。

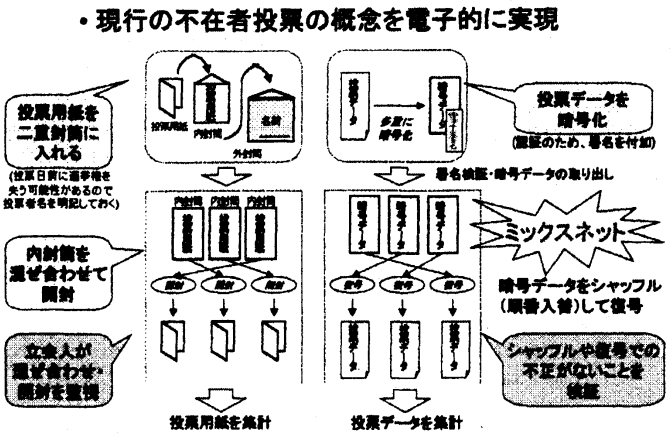

図 1　ミックスネットを用いた電子投票方式

不在者投票では投票用紙を封筒に入れた後、さらに封筒に入れ、外封筒に投票者名を記名する。選挙当日に、投票者名を確認した後、外封筒を取り去り、すべての内封筒を混ぜ合わせる。このようにして外封筒と内封筒の対応をわからなくした後、内封筒を開封して集計をする。投票用紙を内封筒に入れることが暗号化、外封筒に記名することがデジタル署名、封筒を混ぜ合わせて開封するところがミックスネットの処理に相当する。

4．ミックスネットの実現方法

では電子的にどのように、「封筒を混ぜ合わせて開封」するのであろうか。以下、電子投票での利用を想定して説明を続ける。

4.1 シャッフル処理

開封は、暗号文を復号することに相当するので、電子データの混ぜ合わせ（シャッフル）について述べる。外見は全く同一な物理的な封筒と異なり、暗号データはそれぞれビットパターンの異なるデータである。またコンピュータはシャッフル前の電子データとシャッフル後の電子データを正確に記録しておけるので、単なる順番入れ替えではビットパターンの照合で、どの電子データがシャッフル後にどの位置に移動したかが容易に判明してしまう。したがって、シャッフル前後の対応を秘匿するためには、前後でビットパターンそのものを変更する必要がある。それも、封筒の「中身」を変えずに。

これを可能にするために、従来のRSA暗号のように平文と暗号文が１対１に対応するような方式ではなく、確率暗号と呼ばれる暗号方式を採用する。これは一つの平文に対して複数の暗号文が存在する方式である。したがって、封筒の「中身」、すなわち平文を変えずにビットパターンを変えるためには、ある暗号文を、同じ復号文になる別の暗号文に変換してやればよい。この処理を、以下では「再暗号」と呼ぶ。具体的に、ElGamal 暗号での例を紹介する。

ElGamal暗号では、法pにおける素数位数qの部分群の生成元gを用い、乱数xに対して公開鍵を(p, q, g, $y=g^x \bmod p$)とする。メッセージmの暗号化はこの公開鍵と乱数rを用いて、$c=(g^r \bmod p,\ m \cdot y^r \bmod p)$とする。暗号文$c=(c_1, c_2)$を復号するためには、秘密鍵xを用いて、$c_2/c_1^x \bmod p$を計算すれば、メッセージmが入手できる。暗号文はメッセージの約2倍の長さになっているが、暗号時に用いる乱数を変えることで、同じメッセージでも異なる暗号文表現が可能である。次に、暗号文$c=(c_1, c_2)$を、同じ復号文mになるような別の暗号文に変換する再暗号処理について説明する。これは、乱数sを取り、$c'=(c_1 \cdot g^s \bmod p,\ c_2 \cdot y^s \bmod p)$ とすればよい。この結果、c'も同じメッセージmに復号される。なお、ElGamal暗号の特徴はこの再暗号処理を秘密鍵を用いずに実行できる点である。また、このように再暗号処理をした結果、元の暗号文との対応を秘匿できることも知られている。また、二つのElGamal暗号文{c, d}とそれぞれを再暗号した暗号文の対{e, f}が与えられて、どちらの再暗号文がどちらの暗号文に再暗号処理したものなのかを判定することが困難であることが知られている。すなわち、再暗号処理をすれば、シャッフルの対応を秘匿できるのである。

例えば電子投票に用いる場合、投票の秘密は投票センタにも知られたくない。しかし前述したようにコンピュータではどのように順番を並び替えたか、またどの乱数を用いて各暗号文を再暗号したかを記憶しておくことができる。このコンピュータにアクセスできる人にとっては、シャッフル前後の対応が判明してしまう。そこで、複数のサーバ（コンピュータ）を用いて、シャッフルを逐次的に行うことが想定されている。

4.2 開封処理

次に、開封処理について述べる。せっかくシャッフルをしていても、復号鍵を所有している人がシャッフル前の暗号データを直接復号してしまえば、誰が何に投票したかがわかってしまう。そこで、復号鍵もシャッフルのように複数のサーバで行うことを考える。シャッフルと復号の形態で2つの方式が考えられる。すなわち

- ワンパス方式
- ツーパス方式

である。ワンパス方式は各サーバでシャッフルしつつ復号処理もする方式である。各サーバで処理が終わった後はミックスネットの出力であるところのシャッフルされた復号結果が得られる（図2）。

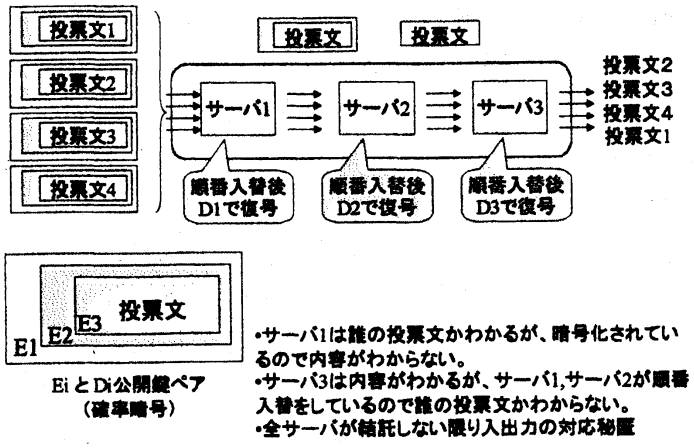

図 2 ワンパス方式

ツーパス方式は、まず、各サーバでシャッフルを行った後、その結果を複数のサーバが共同で復号する方式である。この方式では、復号処理がシャッフルと独立におこなわれるため、任意の group decryption の技術が採用できる（図３）。

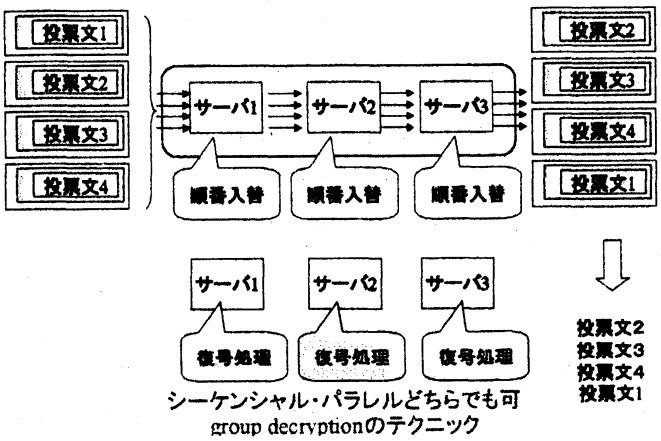

図 3 ツーパス方式

なお、図２、図３では入力の暗号文があたかも３つの公開鍵で暗号化されているように表現されているが、必ずしも暗号化処理を３回行う必要があるものではない。たとえば、ElGamal 暗号では、それぞれのサーバの公開鍵を y_1, y_2, y_3 とすると、合成した公開鍵 $y = y_1 \cdot y_2 \cdot y_3$ で暗号化処理を一回行うだけで３つのサーバでしか復号できない暗号文を生成することができる。

５．ミックスネットの正当性保証方法

電子投票の不正集計防止の要件を満たすためには、なんらかの形でミックスネットの出力の正しさを保証する必要がある。そのために、ミックスネットの検証性(verifiability)を確保するさまざま手段が研究されてきた。大きく分けてゼロ知識証明を利用して誰でも検証できるようにする方式と、それより手軽な計算量で、ミックスネット内のサーバ間で相互に検証する方式である。

5.1 ゼロ知識証明を利用した方式

ゼロ知識証明は、計算量は多いものの、誰でもミックスネットの正当性を確認できるという点で最も強力な正当性保証方法である。そこで、ミックスネットに特化して、なんとか計算量を減らせないかという研究がされている。上述のように、ミックスネットの処理はシャッフルと復号の２つに大別できる。復号処理は group decryption などの既存の技術で効率のよい正当性保証の方法が提案されている。そこで、シャッフルの正当性保証の方法に注目が集まっている。当初は 1995 年に Sako-Kilian の cut-and-choose 法と呼ばれるゼロ知識証明テクニックを用いたシャッフルの正当性保証の方式が提案されたが、入力される暗号文の数ｎに対して 640ｎ回のべき乗剰余演算が必要で、現実的とは思われなかった。次に 1999 年に Abe により、シャッフルを複数の置換回路に置き換えて証明する permutation-network 法が提案された。これは 7ｎlogｎのべき乗剰余演算で証明が可能である。さらに 2001 年にはいって、Furukawa-Sako により、シャッフルを表現する置換行列の性質を利用した証明方法が提案された。これは 18ｎ回のべき乗剰余演算でシャッフルの正当性が保証できる。また、同年 Neff が多項式法と呼ばれる証明方法を提案した。これは (x-a)(x-b)(x-c)の多項式が、a,b,c を入れ替えても不変であることを示す 7move のゼロ知識証明である。当初は 42ｎ回のべき乗剰余演算が必要であったが、2003 年 Groth が 12ｎ回のべき乗剰余演算で計算できるように改良した。

5.2 サーバ間検証を利用した方式

ミックスネット内のサーバで相互に検証を行い、ゼロ知識証明を使うよりも少ない演算量で正当性を保証する方式についての研究も行われている。しかし、ゼロ知識証明という安全性の指標が確立している手法と比較して、サーバ間の信頼モデルをどう構成するか、どのような性質が満たされていれば充分安全であるかいえるか、という検討が遅れている分野でもある。したがって、Practical Mix (Eurocrypt 98) や Flash Mixing (PODC99)，Optimistic Mixing(Asiacrypt02)というさまざまな方式が提案されているが、いずれも脆弱性が指摘されている。たとえば、Optimisitc Mixing では、シャッフル全体の正当性を示すのではなく、部分的な一致、たとえばシャッフル前データの CRC とシャッフル後のデータの CRC が等しいことを示すのみとし、復号後に正しい Message authentication code が復元されるかどうかで不正の有無を確認するというアイディアで構成れている。しかし、これは最初と最後のサーバが結託する不正に弱いことを Abe らが発表している。また、不正の種類も、特定の入力に対する出力の対応が類推できてしまうものなのか、偽りの出力

を出しても検出されないものなのか、偽りの出力が検出されても、不正者を特定できないようにするものなのか、はたまた、なにも出力されないようにするものなのか、とさまざまである。

6．おわりに

電子投票への適用を例に、ミックスネットについて議論した。ミックスネットの正当性保証については、強力なゼロ知識証明を用いて保証する方式が主流であり、実際、より効率面で改良された手法が近年提案されている。一方、安全性が明確に定式化されれば、より効率のよいミックスネットを構成できる可能性がある。ミックスネットを定式化し、攻撃モデルや安全性を厳密に定義することはチャレンジングな課題であると思われる。

参考文献

- D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, Vol. 24, No. 2, pp. 84-88, (1981).
- C. Park, K. Itoh, and K. Kurosawa, Efficient Anonymous Channel and All/Nothing Election Scheme. EUROCRYPT 1993, pp. 248-259 (1993).
- K. Sako and J. Kilian. Receipt-free mix-type voting scheme -A practical solution to the implementation of voting booth. Eurocrypt '95, LNCS 921, pp. 393-403 (1995).
- M. Jakobsson. A practical mix. Eurocrypt '98, LNCS 1403, pp. 448-461 (1998).
- M. Abe. Mix-Networks on Permutation Networks. ASIACRYPT '99, LNCS 1716, pp. 258-273, Springer-Verlag, (1999).
- M. Jakobsson. "Flash Mixing", PODC '99
- A. Juels and M. Jakobsson. An optimally robust hybrid mix network. Proc. of the 20th annual ACM Symposium on Principles of Distributed Computation, 2001
- J. Furukawa and K. Sako. An Efficient Scheme for Proving a Shuffle. CRYPTO 2001, LNCS 2139 pp. 368-387 (2001).
- C. A. Neff. A Verifiable Secret Shuffle and its Application to E-Voting, ACMCCS 01 pp. 116-125 (2001).
- P. Golle, S. Zhong, D. Boneh, M. Jakobsson, and A. Juels. Optimistic mixing for exit-polls, Asiacrypt 2002, LNCS 2501, pp. 451-465 (2002)
- J. Furukawa, K. Mori, S. Obana, and K. Sako. An Implementation of a Universally Verifiable Electronic Voting Scheme based on Shuffling. Financial Cryptography 2002.
- J. Groth. A Verifiable Secret Shuffle of Holomorphic Encryptions. Public Key Cryptography — PKC 2003, LNCS 2567 pp. 145-160 (2003)

- M. Abe and H. Imai. Breaking Some Robust Mix-nets. Proceedings of the 2003 Symposium on Cryptography and Information Security, pp. 497-502
- M. Ohkubo and M . Abe. A length-invariant hybrid mix. Asiacrypt 2000, LNCS 1976, pp. 178-191 (2000)
- W. Ogata, K. Kurosawa, K. Sako, and K. Takatani. Fault tolerant anonymous channel. 1st International Conference on Information and Communications Security. ICICS, LNCS 1334, pp. 440-444 (1997).